CLAIMS

1. A method of providing electronic data from a first computer to a second computer, the method comprising the steps of:

1: at least partially encrypting the data with an encryption key (K_s) in the first computer, said encryption key (K_s) having a corresponding decryption key (K_d),

2: communicating the at least partially encrypted data from the first computer to the second computer,

3: the second computer requesting the decryption key (K_d) from the first computer,

4: the first computer providing the decryption key (K_d) to the second computer,

5: the second computer decrypting the at least partially encrypted data using the decryption key (K_d),

6: rendering the decryption key (K_d) unfit for use,

7: outputting the data to an output device.

2. A method according to claim 1, wherein step 2 further comprises the step of branding the at least partially encrypted data with an identifier (I_u) in the first computer, and wherein step 3 is performed by the second computer providing the identifier (I_u).

3. A method according to claim 1, wherein step 6 comprises deleting the decryption key (K_d) from the second computer after step 5 has been performed.

4. A method according to claim 1, wherein step 6 comprises storing the decryption key (K_d) in a volatile memory of the second computer only.

5. A method according to claim 1, wherein step 4 comprises the steps of

- determining whether the second computer fulfils one or more predetermined criteria selected from a group of criteria,
- providing the decryption key (K_d) only if the second computer fulfils one or more of said predetermined criteria.

6. A method according to claim 5, wherein the determining step comprises determining whether the second computer fulfils one or more criteria selected from the group of criteria consisting of,

- the time elapsed between the encryption of the data and the request for the decryption key (K_d) does not exceed a predetermined time interval,
- the decryption key (K_d) has not been requested more than a predetermined number of times,
- the second computer is a predetermined computer,
- valid payment has been provided,
- the hardware being used by the second computer is a predetermined hardware,
- the e-mail address of the user is a predetermined e-mail address,
- the user name of the user is a predetermined user name,
- the output device is a predetermined type of output device,
- the output device driver is a predetermined output device driver,
- the network ID is a predetermined network ID.

7. A method according to claim 1, wherein step 1 is performed using a random secret encryption key.

8. A method according to claim 1, wherein step 4 is performed using an encrypted session between the first computer and the second computer.

9. A method according to claim 1, wherein step 7 is performed by dividing the at least partially encrypted data into a number of subparts, each subpart in turn being output to an output device.

10. A method according to claim 9, wherein step 7 is performed at least substantially simultaneously with step 5, in such a way that each subpart of the data is in turn decrypted and output to the output device.

11. A method according to claim 10, wherein step 7 is performed by streaming the data to the output device.

12. A method according to claim 1, further comprising the step of providing payment to the first computer.

13. A method according to claim 12, wherein the step of providing payment comprises the step of charging a credit card.

14. A method according to claim 13, wherein the step of charging a credit card further comprises the steps of:

- entering relevant credit card data,
- the first computer checking whether the corresponding credit card is valid and chargeable.

15. A method according to claim 1, further comprising the steps of:

a: the second computer re-requesting the decryption key (K_d),

b: the first computer providing the decryption key (K_d) to the second computer,

c: the second computer decrypting the at least partially encrypted data,

d: rendering the decryption key (K_d) unfit for use,

e: outputting the data to an output device.

16. A method according to claim 15, wherein step d comprises deleting the decryption key (K_d) from the second computer after the data has been output to the output device.

17. A method according to claim 15, further comprising the step of providing payment to the first computer.

18. A method according to claim 17, wherein the step of providing payment comprises the step of charging a credit card.

19. A method according to claim 18, wherein the step of charging a credit card further comprises the steps of:

- entering relevant credit card data,
- the first computer checking whether the corresponding credit card is valid and chargeable.

20. A method according to claim 1, comprising the step of providing electronic data from a server device to a client device.

21. A method according to claim 1, further comprising the steps of:

- the first computer requesting additional information from the second computer,
- the second computer providing said additional information,

- the first computer using said additional information for determining whether to provide the decryption key (K_d) or not.

22. A method according to claim 21, wherein the step of the second computer providing said additional information comprises the step of the user providing at least some of said additional information.

23. A computer program system for providing electronic data from a first computer to a second computer, the computer program system being adapted to:

1: at least partially encrypt the data with an encryption key (K_s) in the first computer, said encryption key (K_s) having a corresponding decryption key (K_d),

2: communicate the at least partially encrypted data from the first computer to the second computer,

3: provide a request for the decryption key (K_d) from the second computer to the first computer,

4: cause the first computer to provide the decryption key (K_d) to the second computer,

5: cause the second computer to decrypt the at least partially encrypted data using the decryption key (K_d),

6: render the decryption key (K_d) unfit for use,

7: output the data to an output device.

24. A computer readable data carrier loaded with a computer program system for providing electronic data from a first computer to a second computer, the computer program system being adapted to:

1: at least partially encrypt the data with an encryption key (K_s) in the first computer, said encryption key (K_s) having a corresponding decryption key (K_d),

2: communicate the at least partially encrypted data from the first computer to the second computer,

3: provide a request for the decryption key (K_d) from the second computer to the first computer,

4: cause the first computer to provide the decryption key (K_d) to the second computer,

5: cause the second computer to decrypt the at least partially encrypted data using the decryption key (K_d),

6: render the decryption key (K_d) unfit for use,

7: output the data to an output device.

25. A computer system operatively connected to a computer readable data carrier loaded with a computer program system for providing electronic data from a first computer of the computer system to a second computer of the computer system, the computer system and the program system being adapted to:

1: at least partially encrypt the data with an encryption key (K_s) in the first computer, said encryption key (K_s) having a corresponding decryption key (K_d),

2: communicate the at least partially encrypted data from the first computer to the second computer,

3: provide a request for the decryption key (K_d) from the second computer to the first computer,

4: cause the first computer to provide the decryption key (K_d) to the second computer,

5: cause the second computer to decrypt the at least partially encrypted data using the decryption key (K_d),

6: render the decryption key (K_d) unfit for use,

7: output the data to an output device.

26. A method of providing electronic data from a first computer to a second computer, the method comprising the steps of:

1: at least partially encrypting the data with an encryption key (K_s) in the first computer, said encryption key (K_s) having a corresponding decryption key (K_d),

2: the second computer requesting the decryption key (K_d) from the first computer,

3: the first computer providing the decryption key (K_d) to the second computer,

4: communicating the at least partially encrypted data from the first computer to the second computer,

5: the second computer concurrently receiving and decrypting, by means of a decryption computer program, the at least partially encrypted data, and outputting the data to a selected data output computer program for outputting a signal representative of the decrypted data to a selected software program or hardware device, the data output computer program being known to render the decrypted data unfit for use after output thereof to the selected software program or hardware device,

6: rendering the decrypted data unfit for use.

27. A method according to claim 26, further comprising the step of rendering the decryption key (K_d) unfit for use.

28. A method according to claim 26, wherein step 6 is performed concurrently with step 5.

29. A method according to claim 27, wherein the step is performed by deleting the decryption key (K_d) from the second computer after step 5 has been performed.

30. A method according to claim 26, wherein step 5 comprises the steps of:
- dividing the at least partially encrypted data into a number of subparts,
- decrypting each subpart in turn,
- outputting each subpart in turn to the selected data output computer program,
- outputting a signal representative of each subpart in turn to the selected software program or hardware device,

and wherein step 6 comprises the step of:
- rendering each subpart unfit for use after it has been output to the selected data output computer program.

31. A method according to claim 30, wherein each subpart is rendered unfit for use before the subsequent subpart is decrypted.

32. A method according to claim 26, wherein step 5 is performed by outputting the data to a printer device using a printer driver, the printer driver being of a type being known to render the data unfit for use after output thereof to the printer device.

33. A method according to claim 26, wherein step 3 comprises the steps of:
- determining whether the second computer fulfils one or more predetermined criteria selected from a group of criteria,
- providing the decryption key (K_d) only if the second computer fulfils one or more of said predetermined criteria.

34. A method according to claim 33, wherein the determining step comprises determining whether the second computer fulfils one or more criteria selected from the group of criteria consisting of,

- the time elapsed between the encryption of the data and the request for the decryption key (K_d) does not exceed a predetermined time interval,
- the decryption key (K_d) has not been requested more than a predetermined number of times,
- the second computer is a predetermined computer,
- valid payment has been provided,
- the hardware being used by the second computer is a predetermined hardware,
- the e-mail address of the user is a predetermined e-mail address,
- the user name of the user is a predetermined user name,
- the output device is a predetermined type of output device,
- the output device driver is a predetermined output device driver,
- the network ID is a predetermined network ID.

35. A method according to claim 26, wherein the output device is a printer, and wherein the data is streamed from the second computer to the printer via the selected data output computer program.

36. A computer program system of providing electronic data from a first computer to a second computer, the computer program system being adapted to:

1: at least partially encrypt the data with an encryption key (K_s) in the first computer, said encryption key (K_s) having a corresponding decryption key (K_d),

2: cause the second computer to request the decryption key (K_d) from the first computer,

3: cause the first computer to provide the decryption key (K_d) to the second computer,

4: communicate the at least partially encrypted data from the first computer to the second computer,

5: cause the second computer to concurrently receive and decrypt, by means of a decryption computer program, the at least partially encrypted data, and output the data to a selected data output computer program for outputting a signal representative of the decrypted data to a selected software program or hardware device, and cause the data output computer program to render the decrypted data unfit for use after output thereof to the selected software program or hardware device,

6: render the decrypted data unfit for use.

37. A computer readable data carrier loaded with a computer program system of providing electronic data from a first computer to a second computer, the computer program system being adapted to:

1: at least partially encrypt the data with an encryption key (K_s) in the first computer, said encryption key (K_s) having a corresponding decryption key (K_d),

2: cause the second computer to request the decryption key (K_d) from the first computer,

3: cause the first computer to provide the decryption key (K_d) to the second computer,

4: communicate the at least partially encrypted data from the first computer to the second computer,

5: cause the second computer to concurrently receive and decrypt, by means of a decryption computer program, the at least partially encrypted data, and output the data to a selected data output computer program for outputting a signal representative of the decrypted data to a selected software program or hardware device, and cause the data output computer program to render the decrypted data unfit for use after output thereof to the selected software program or hardware device,

6: render the decrypted data unfit foruse.

38. A computer system operatively connected to a computer readable data carrier loaded with a computer program system of providing electronic data from a first computer of the computer system to a second computer of the computer system, the computer system and the computer program system being adapted to:

1: at least partially encrypt the data with an encryption key (K_s) in the first computer, said encryption key (K_s) having a corresponding decryption key (K_d),

2: cause the second computer to request the decryption key (K_d) from the first computer,

3: cause the first computer to provide the decryption key (K_d) to the second computer,

4: communicate the at least partially encrypted data from the first computer to the second computer,

5: cause the second computer to concurrently receive and decrypt, by means of a decryption computer program, the at least partially encrypted data, and output the data to a selected data output computer program for outputting a signal representative of the decrypted data to a selected software program or hardware device, and cause the data

output computer program to render the decrypted data unfit for use after output thereof to the selected software program or hardware device,

6: render the decrypted data unfit for use.

39. A computer system for providing electronic data comprising

- a first computer,
- a second computer,
- an output device,

the first computer comprising

- encryption means for at least partially encrypting data with an encryption key (K_s), said encryption key (K_s) having a corresponding decryption key (K_d),
- first communication means for communicating the at least partially encrypted data to the second computer,
- providing means for providing the decryption key (K_d) to the second computer on request,

the second computer comprising

- second communication means for receiving the at least partially encrypted data from the first computer,
- requesting and receiving means for requesting and receiving the decryption key (K_d) from the first computer,
- decryption means for decrypting the at least partially encrypted data,
- outputting means for outputting the data to the output device,
- means for rendering the decryption key (K_d) unfit for use.

40. A computer system according to claim 39, wherein the means for rendering the decryption key (K_d) unfit for use comprises deleting means for deleting the decryption key (K_d) after the data has been decrypted.

41. A computer system according to claim 39, wherein the first computer is a server device and the second computer is a client device.

42. A computer system according to claim 39, wherein the first communication means comprises a global computer network.

43. A computer system according to claim 39, wherein the second communication means comprises a global computer network.

44. A computer system according to claim 39, wherein the first computer further comprises means for receiving payment.

45. A computer system according to claim 44, wherein the means for receiving payment comprises means for checking the validity and chargeability of a credit card.

46. A computer system according to claim 39, wherein the outputting means for outputting the data to the output device comprises a data output computer program for outputting a signal representative of the decrypted data to a selected software program or hardware device, the data output computer program being known to render the decrypted data unfit for use after output thereof to the selected software program or hardware device.

47. A method of transferring data from a computer system to an output device, the computer system comprising a first computer and a plurality of second computers, said first computer and said second computers being interconnected via a computer network, the data being present at at least one of the second computers, the method comprising the steps of:

1: sending, by means of said at least one second computer, a request to the first computer for permission to output the data to the output device, said request including an identification of the output device,

2: checking, by means of the first computer, whether the output device is an allowed type of output device,

3: the first computer providing an answer to the request to the second computer, the answer including a permission to output the data to the output device if the output device is of an allowed type,

4: if the output device is of an allowed type: outputting the data from the second computer to the output device.

48. A method according to claim 47, wherein step 2 is performed by, by means of the first computer, comparing the type of output device with a predefined positive list of allowed types of output devices, and wherein the answer of step 3 includes a permission to output

the data to the output device only if the type of output device is present on said predefined positive list.

49. A method according to claim 47, wherein step 2 is performed by, by means of the first computer, comparing the type of output device with a predefined negative list of not-allowed types of output devices, and wherein the answer of step 3 includes a permission to output the data to the output device only if the type of output device is not present on said predefined negative list.

50. A method according to claim 47, wherein step 2 is performed by, by means of the first computer, checking whether the output device comprises an allowed type of hardware.

51. A method according to claim 47, wherein step 2 is performed by, by means of the first computer, checking whether the output device comprises an allowed type of output driver.

52. A method according to claim 47, wherein the answer of step 3 further includes a decryption key for decrypting encrypted electronic data.

53. A method according to claim 47, the output device comprising a printer, wherein step 4 is performed by printing the data using the printer.

54. A method according to claim 47, wherein the request of step 1 includes an identification of the driver of the output device.

55. A computer program system for transferring data from a computer system to an output device, the computer system comprising a first computer and a plurality of second computers, said first computer and said second computers being interconnected via a computer network, the data being present at at least one of the second computers, the computer program system being adapted to:

1: send, by means of said at least one second computer, a request to the first computer for permission to output the data to the output device, said request including an identification of the output device,

2: check, by means of the first computer, whether the output device is an allowed type of output device,

3: cause the first computer to provide an answer to the request to the second computer, the answer including a permission to output the data to the output device if the output device is of an allowed type,

4: if the output device is of an allowed type: output the data from the second computer to the output device.

56. A computer readable data carrier loaded with a computer program system for transferring data from a computer system to an output device, the computer system comprising a first computer and a plurality of second computers, said first computer and said second computers being interconnected via a computer network, the data being present at at least one of the second computers, the computer program system being adapted to:

1: send, by means of said at least one second computer, a request to the first computer for permission to output the data to the output device, said request including an identification of the output device,

2: check, by means of the first computer, whether the output device is an allowed type of output device,

3: cause the first computer to provide an answer to the request to the second computer, the answer including a permission to output the data to the output device if the output device is of an allowed type,

4: if the output device is of an allowed type: output the data from the second computer to the output device.

57. A computer system operatively connected to a computer readable data carrier loaded with a computer program system for transferring data from a computer system to an output device, the computer system comprising a first computer and a plurality of second computers, said first computer and said second computers being interconnected via a computer network, the data being present at at least one of the second computers, the computer system and the computer program system being adapted to:

1: send, by means of said at least one second computer, a request to the first computer for permission to output the data to the output device, said request including an identification of the output device,

2: check, by means of the first computer, whether the output device is an allowed type of output device,

3: cause the first computer to provide an answer to the request to the second computer, the answer including a permission to output the data to the output device if the output device is of an allowed type,

4: if the output device is of an allowed type: output the data from the second computer to the output device.

58. A method of providing electronic data from a first computer to a second computer, the second computer comprising an output device, the method comprising the steps of:

1: at least partially encrypting the data with an encryption key (K_s) in the first computer, said encryption key (K_s) having a corresponding decryption key (K_d),

2: communicating the at least partially encrypted data from the first computer to the second computer,

3: the second computer requesting the decryption key (K_d) from the first computer,

4: checking whether the driver of the output device is an allowed type of driver,

5: the first computer providing the decryption key (K_d) to the second computer only if said driver is an allowed type of driver,

6: the second computer decrypting the at least partially encrypted data in case said decryption key (K_d) is provided,

7: outputting the decrypted data to the output device.

59. A method according to claim 58, wherein the output device is a printer, and wherein step 7 is performed by printing the data.

60. A method according to claim 58, wherein step 4 is performed by comparing the type of driver with a predefined positive list of allowed types of drivers, and wherein step 5 is only performed if the driver is of a type which is present on said predefined positive list.

61. A method according to claim 58, wherein step 4 is performed by comparing the type of driver with a predefined negative list of not-allowed types of drivers, and wherein step 5 is only performed if the driver is of a type which is not present on said predefined negative list.

62. A method according to claim 58, further comprising the step of rendering the decryption key (K_d) unfit for use.

63. A method according to claim 62, wherein the step of rendering the decryption key (K_d) unfit for use comprises deleting the decryption key (K_d) from the second computer after step 6 has been performed.

64. A method according to claim 62, wherein the step of rendering the decryption key (K_d) unfit for use comprises storing the decryption key (K_d) in a volatile memory of the second computer only.

65. A method according to claim 58, further comprising the steps of:

- the second computer concurrently receiving and decrypting, by means of a decryption computer program, the at least partially encrypted data, and outputting the data to a selected data output computer program for outputting a signal representative of the decrypted data to a selected software program or hardware device, the data output computer program being known to render the decrypted data unfit for use after output thereof to the selected software program or hardware device,
- rendering the decrypted data unfit for use.

66. A method according to claim 58, further comprising the steps of:

a: the second computer re-requesting the decryption key (K_d),

b: checking whether the driver of the output device is an allowed type of driver,

c: the first computer providing the decryption key (K_d) to the second computer only if said driver is an allowed type of driver,

d: the second computer decrypting the at least partially encrypted data in case said decryption key (K_d) is provided,

e: outputting the decrypted data to the output device.

67. A method according to claim 66, further comprising the step of, by means of a counter, counting the number of times the decryption key (K_d) has been provided to the first computer, said counting step being performed by augmenting said counter each time the decryption key (K_d) has been provided to the first computer, step c being performed only if the number of times the decryption key (K_d) has previously been requested does not exceed a predetermined number of times.

68. A method according to claim 58, further comprising the steps of:

- determining whether the second computer fulfils one or more predetermined criteria selected from a group of criteria,
- providing the decryption key (K_d) only if the second computer fulfils one or more of said predetermined criteria.

69. A method according to claim 68, wherein the determining step comprises determining whether the second computer fulfils one or more criteria selected from the group of criteria consisting of,

- the time elapsed between the encryption of the data and the request for the decryption key (K_d) does not exceed a predetermined time interval,
- the decryption key (K_d) has not been requested more than a predetermined number of times,
- the second computer is a predetermined computer,
- valid payment has been provided,
- the hardware being used by the second computer is a predetermined hardware,
- the e-mail address of the user is a predetermined e-mail address,
- the user name of the user is a predetermined user name,
- the network ID is a predetermined network ID.

70. A computer program system for providing electronic data from a first computer to a second computer, the second computer comprising an output device, the computer program system being adapted to:

1: at least partially encrypt the data with an encryption key (K_s) in the first computer, said encryption key (K_s) having a corresponding decryption key (K_d),

2: communicate the at least partially encrypted data from the first computer to the second computer,

3: cause the second computer to request the decryption key (K_d) from the first computer,

4: check whether the driver of the output device is an allowed type of driver,

5: cause the first computer to provide the decryption key (K_d) to the second computer only if said driver is an allowed type of driver,

6: cause the second computer to decrypt the at least partially encrypted data in case said decryption key (K_d) is provided,

7: output the decrypted data to the output device.

71. A computer readable data carrier loaded with a computer program system for providing electronic data from a first computer to a second computer, the second computer comprising an output device, the computer program system being adapted to:

1: at least partially encrypt the data with an encryption key (K_s) in the first computer, said encryption key (K_s) having a corresponding decryption key (K_d),

2: communicate the at least partially encrypted data from the first computer to the second computer,

3: cause the second computer to request the decryption key (K_d) from the first computer,

4: check whether the driver of the output device is an allowed type of driver,

5: cause the first computer to provide the decryption key (K_d) to the second computer only if said driver is an allowed type of driver,

6: cause the second computer to decrypt the at least partially encrypted data in case said decryption key (K_d) is provided,

7: output the decrypted data to the output device.

72. A computer system operatively connected to a computer readable data carrier loaded with a computer program system for providing electronic data from a first computer to a second computer, the second computer comprising an output device, the computer system and the computer program system being adapted to:

1: at least partially encrypt the data with an encryption key (K_s) in the first computer, said encryption key (K_s) having a corresponding decryption key (K_d),

2: communicate the at least partially encrypted data from the first computer to the second computer,

3: cause the second computer to request the decryption key (K_d) from the first computer,

4: check whether the driver of the output device is an allowed type of driver,

5: cause the first computer to provide the decryption key (K_d) to the second computer only if said driver is an allowed type of driver,

6: cause the second computer to decrypt the at least partially encrypted data in case said decryption key (K_d) is provided,

7: output the decrypted data to the output device.

73. A method of decrypting data, the method utilising a hardware processor containing an inaccessible part, the method comprising, by means of said hardware processor:

- storing, in the hardware processor, an encryption/decryption key (AB) comprising a public part (A) and a corresponding private part (B), the private part (B) of the key (AB) being stored in the inaccessible part of the hardware processor,
- outputting the public part (A) of the key (AB) to an external processor or program,
- receiving, from said external processor, an encrypted decryption key (E) which is encrypted by means of the public part (A) of the key (AB),
- decrypting key (E) into the inaccessible part of the hardware processor by using the private part (B),
- receiving data encrypted with encryption key (E),
- decrypting the data using the decrypted key (E),
- outputting the decrypted data.

74. A method according to claim 73, wherein the outputting step is performed by outputting the decrypted data to an output device.

75. A method according to claim 73, further comprising the step of encrypting the key (E) externally to the hardware processor.

76. A method according to claim 73, further comprising the step of encrypting the data with an encryption key corresponding to the decryption key (E) externally to the hardware processor.

77. A method according to claim 73, further comprising the step of, by means of the hardware processor, generating and storing the encryption/decryption key (AB) in the hardware processor.

78. A method according to claim 73, further comprising the step of rendering the decryption key (E) unfit for use after the data has been decrypted.

79. A method according to claim 78, wherein the step of rendering the decryption key (E) unfit for use comprises deleting the decryption key (E) from the hardware processor.

80. A computer program system for decrypting data, the computer program system being adapted to co-operate with a hardware processor containing an inaccessible part, the

computer program system being further adapted to, in co-operation with the hardware processor:

- store, in the hardware processor, an encryption/decryption key (AB) comprising a public part (A) and a corresponding private part (B), the private part (B) of the key (AB) being stored in the inaccessible part of the hardware processor,
- output the public part (A) of the key (AB) to an external processor or program,
- receive, from said external processor, an encrypted decryption key (E) which is encrypted by means of the public part (A) of the key (AB),
- decrypt key (E) into the inaccessible part of the hardware processor by using the private part (B),
- receive data encrypted with encryption key (E),
- decrypt the data using the decrypted key (E),
- output the decrypted data.

81. A computer readable data carrier loaded with a computer program system for decrypting data, the computer program system being adapted to co-operate with a hardware processor containing an inaccessible part, the computer program system being further adapted to, in co-operation with the hardware processor:

- store, in the hardware processor, an encryption/decryption key (AB) comprising a public part (A) and a corresponding private part (B), the private part (B) of the key (AB) being stored in the inaccessible part of the hardware processor,
- output the public part (A) of the key (AB) to an external processor or program,
- receive, from said external processor, an encrypted decryption key (E) which is encrypted by means of the public part (A) of the key (AB),
- decrypt key (E) into the inaccessible part of the hardware processor by using the private part (B),
- receive data encrypted with encryption key (E),
- decrypt the data using the decrypted key (E),

output the decrypted data.

82. A computer system operatively connected to a computer readable data carrier loaded with a computer program system for decrypting data, the computer system and the computer program system being adapted to co-operate with a hardware processor containing an inaccessible part, the computer system and the computer program system being further adapted to, in co-operation with the hardware processor:

- store, in the hardware processor, an encryption/decryption key (AB) comprising a public part (A) and a corresponding private part (B), the private part (B) of the key (AB) being stored in the inaccessible part of the hardware processor,
- output the public part (A) of the key (AB) to an external processor or program,
- receive, from said external processor, an encrypted decryption key (E) which is encrypted by means of the public part (A) of the key (AB),
- decrypt key (E) into the inaccessible part of the hardware processor by using the private part (B),
- receive data encrypted with encryption key (E),
- decrypt the data using the decrypted key (E),
- output the decrypted data.

83. An electronic processor containing an inaccessible part, and being adapted to, in co-operation with a computer program system, to decrypt data and to:

- store, in the hardware processor, an encryption/decryption key (AB) comprising a public part (A) and a corresponding private part (B), the private part (B) of the key (AB) being stored in the inaccessible part of the hardware processor,
- output the public part (A) of the key (AB) to an external processor or program,
- receive, from said external processor, an encrypted decryption key (E) which is encrypted by means of the public part (A) of the key (AB),
- decrypt key (E) into the inaccessible part of the hardware processor by using the private part (B),
- receive data encrypted with encryption key (E),
- decrypt the data using the decrypted key (E),
- output the decrypted data.

84. A method of distributing electronic data via a computer network, said electronic data originating from a plurality of publishers, the method comprising the steps of:

1: each of the plurality of publishers making electronic data available from a first computer being connected to the computer network,

2: the first computer distributing electronic data to users on demand, and

3: the first computer controlling the usage of the electronic data being made available to each user.

85. A method according to claim 84, wherein step 3 is performed by counting the number of times the electronic data has been made available, and wherein usage of the data is prevented or limited in case said number of times exceeds a predetermined number of times.

86. A method according to claim 84, wherein step 3 comprises the steps of:

- at least partially encrypting the data with an encryption key (K_s) in the first computer prior to distributing the data, so that the data is distributed in an encrypted form, said encryption key (K_s) having a corresponding decryption key (K_d),
- the user requesting the decryption key (K_d),
- the first computer providing the decryption key (K_d) to the user,
- decrypting the at least partially encrypted data using the decryption key (K_d),
- rendering the decryption key (K_d) unfit for use,
- outputting the data to an output device.

87. A method according to claim 86, wherein the step of rendering the decryption key (K_d) unfit for use comprises deleting the decryption key (K_d).

88. A method according to claim 86, wherein the decryption key (K_d) is only provided if the user fulfils one or more predetermined criteria selected from a group of criteria.

89. A method according to claim 88, wherein the group of criteria consists of:

- the time elapsed between the encryption of the data and the request for the decryption key (K_d) does not exceed a predetermined time interval,
- the decryption key (K_d) has not been requested more than a predetermined number of times,
- the computer used by the user is a predetermined computer,
- valid payment has been provided,
- the hardware being used by the user is a predetermined hardware,
- the e-mail address of the user is a predetermined e-mail address,
- the user name of the user is a predetermined user name,
- the output device being used by the user is a predetermined type of output device,
- the output device driver being used by the user is a predetermined output device driver,
- the network ID is a predetermined network ID.

90. A method according to claim 84, further comprising the steps of:
- the first computer charging each user for the data made available to the user,
- the first computer providing payment to each of the publishers.

91. A method according to claim 90, wherein the amount charged is dependent on the content of the distributed electronic data and on the number of copies made available to the user.

92. A method according to claim 90, wherein the payment to each of the publishers is dependent on the content of the distributed electronic data and on the number of copies being made available to the users.

93. A method according to claim 90, wherein the step of charging each user is performed by charging a credit card of each user.

94. A method according to claim 90, wherein the amount charged is determined by the individual publisher.

95. A method according to claim 90, wherein step 1 is performed by, by means of the first computer, providing a Uniform Resource Locator (URL) corresponding to each piece of electronic data being made available to the respective publisher.

96. A method according to claim 95, wherein the Uniform Resource Locator(s) (URL(s)) is/are placed on a web site belonging to the respective publisher, so as to provide a direct link from said web site to the electronic data.

97. A method according to claim 95, wherein the Uniform Resource Locator(s) (URL(s)) is/are placed on a web site belonging to the owner of the first computer, and wherein step 2 is performed by the user selecting the URL(s) corresponding to the piece(s) of data to which the user wishes to gain access.

98. A method according to claim 84, wherein the electronic data being distributed comprises material to be printed.

99. A method according to claim 84, wherein the electronic data is distributed via a global computer network.

100. A computer program system for distributing electronic data via a computer network, said electronic data originating from a plurality of publishers, the computer program system being adapted to:

1: cause each of the plurality of publishers to make electronic data available from a first computer being connected to the computer network,

2: cause the first computer to distribute electronic data to users on demand, and

3: cause the first computer to control the usage of the electronic data being made available to each user.

101. A computer readable data carrier loaded with a computer program system for distributing electronic data via a computer network, said electronic data originating from a plurality of publishers, the computer program system being adapted to:

1: cause each of the plurality of publishers to make electronic data available from a first computer being connected to the computer network,

2: cause the first computer to distribute electronic data to users on demand, and

3: cause the first computer to control the usage of the electronic data being made available to each user.

102. A computer system operatively connected to a readable data carrier loaded with a computer program system for distributing electronic data via a computer network, said electronic data originating from a plurality of publishers, the computer system and the computer program system being adapted to:

1: cause each of the plurality of publishers to make electronic data available from a first computer being connected to the computer network,

2: cause the first computer to distribute electronic data to users on demand, and

3: cause the first computer to control the usage of the electronic data being made available to each user.